UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,058	01/10/2002	Paul Harry Abbott	GB920010007US1	9940

46320 7590 03/02/2007

CAREY, RODRIGUEZ, GREENBERG & PAUL, LLP
STEVEN M. GREENBERG
950 PENINSULA CORPORATE CIRCLE
SUITE 3020
BOCA RATON, FL 33487

EXAMINER	
SZYMANSKI, THOMAS M	
ART UNIT	**PAPER NUMBER**
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/046,058	**Applicant(s)** ABBOTT, PAUL HARRY	
	Examiner Thomas Szymanski	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 November 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-34 have been examined.

2. Applicant's arguments, see appeal brief, filed 11/07/2006, have been fully considered and are persuasive. The final rejection of 6/07/2006 has been withdrawn.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-2, 4-9, 11-14, 16-24, and 26-31, 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kausik United States Patent Application Publication No. 2001/0008012 (hereinafter "Kausik"), and Bahls et al U.S. Patent No. 5,706,513 (hereinafter "Bahls").

5. Kausik teaches storage of security keys and certificates in a storage means, but fails to explicitly teach fragmenting the keys or certificates. (Kausik Figure 1, paragraphs 11, 24-32)

6. However, in related art, Bahls discloses a system for the storage and fragmentation of files. (Bahls et al Col 5 lines 55-67 – Col 6 lines 1-3, figure 6).

7. As taught by Kausik (paragraph 27) the keys/certificates are stored in any standard storage medium including floppy disks, hard disks, magnetic stripe cards, and smart cards, such media as taught by Bahls is advantageously shared amongst several applications. Wherein the working storage of a given application is not large enough to store an entire data object it is desirable to fragment such a data object into multiple pieces and store those pieces (Bahls Col 1 lines 55-67, Col 2 lines 2-20, Col 3 lines 35-40). Additionally, such fragments when for instance N=2 exists for a given object (key or certificate) and the size is not a multiple of the segment size will be of a non-uniform nature in length when stored and intermixed in the storage medium (Bahls Col 5 lines 55-67).

8. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Bahls with those of Kausik in order to facilitate shared storage amongst applications wherein the working storage of those given applications is not adequate to store an entire working object.

9. Regarding Claims 1, 13, 23: storing a key or a certificate in a storage means (Kausik figure 1, paragraphs 24-32; Bahls figure 6, Col 5 lines 55-67, Col 3 lines 35-40) Kausik teaches storing keys encrypted with a pin in a key wallet.

Fragmenting the key or certificate into non-uniform lengths according to an algorithm (Bahls Col 5 lines 55-67, fig 6) Clearly as taught when a situation exists wherein N=2 and the object size is not a multiple of the segment size the key would be fragmented into pieces of non-uniform length and stored in the associated medium.

Fragments are intermixed with storage means (Bahls figure 7, Col 3 lines 5-17, Col 5 lines 55-67) As provided by the teachings of Bahls and seen in figure 7 the objects are stored amongst each other in shared storage and are therefore intermixed as claimed.

10. Regarding Claim 2: The storage means is a data file (Kausik paragraph 11, 27, figure 1) Kausik states that the implementation dictates a software implementation of storage of the keys, hence the key is clearly stored in a file on a tangible means.

11. Regarding Claim 4: Fragmenting the entity includes fragmenting the bytes (Bahls Col 5 lines 33-66) The division of any digital file has to be in such a manner as to be fragmenting the bytes, since the bytes are what the file is composed of, and the act of fragmenting an object consists of separating it amongst its smaller pieces.

12. Regarding Claim 5: Location of storing fragments is determined by the algorithm (Bahls Col 5 lines 33-67, Col 6 lines 1-3, figures 3, 8) As stated by Bahls the file is fragmented in relation to its storage location since the fragments are created as a purpose of the storage location and furthermore as provided for by the associated key which is stored with the object for recovery.

13. Regarding Claim 6: Algorithm can be used to find the fragments (Bahls Col 5 lines 33-67, Col 6 lines 1-3, figure 8) As stated previously an algorithm must be used to perform such a function and furthermore the implementation of such an algorithm provides for a reciprocal process. The provided key that is stored with the data objects provides for putting the file back together and relates each piece with the next through the fragments of the key.

14. Regarding Claim 7: Storage means has a pass code used by the algorithm (Kausik paragraph 24-26, 37) Kausik provides an encrypted key, that is encrypted by a PIN, that can only be decrypted by use of that same PIN.

15. Regarding Claim 8: Fragments stored at locations determined by pass code (Kausik paragraph 24-26, 37; Bahls Figure 8, Col 3 lines 45-65, Col 6 lines 1-41)

16. Regarding Claim 9: Bit map as a record of fragment locations (Bahls Fig 2, Fig 7) As it can be seen from the figures the Implementation of this system provides for a bit map as a record of fragment locations. During the processing of these files they are staged into queues and as such have formed a map of the actual file since it is no longer together but segmented into bits and thus only represented while staged. These segmented bit patterns provide for the reconstruction of the file upon it's use or the file being placed back into permanent storage.

17. Regarding Claim 11 and 12: the storage means is a keystore repository; the algorithm is implemented as a keystore class (Kausik paragraph 11, figure1; Bahls Col 5 lines 55-67, figure 7-8)

18. Claims 14, 16-24, 26-31, 33-34 are an apparatus and computer program product implementation of the above rejected claims and as such are rejected on the same basis.

19. Claims 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kausik United States Patent Application Publication No. 2001/0008012 (hereinafter

"Kausik"), and Bahls et al U.S. Patent No. 5,706,513 (hereinafter "Bahls") as applied to claim 1 above.

20. Regarding Claim 10: Fragment stored immediately after another if storage location is occupied. It is well known within the art that when implementing an algorithm such as a hash algorithm for the placement of objects amongst potential storage spots that when a collision occurs the object is stored immediately following the occupied spot. Thus Official notice is given that performing such an operation is a well known practice within the art.

21. Claim 32 is a computer program product implementation of the above rejected claim and as such is rejected on the same basis.

22. Claims 3, 15, 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kausik United States Patent Application Publication No. 2001/0008012 (hereinafter "Kausik"), Bahls et al U.S. Patent No. 5,706,513 (hereinafter "Bahls") as applied to claim 1 above, and further in view of Henson et al United States Patent No. 7,003,108 (hereinafter "Henson").

23. The combination of Bahls and Kausik teaches a manner of storing keys and certificates as in claim 1 above and individually teach both the use of nulls (Bahls Col 5 lines 66-67) in storage and as in the case of Kausik random data padded onto a message (Kausik claim 22), but both fail to explicitly teach random bit patterns within the storage means.

24. However, in related art, Henson teaches the use of random characters for padding. Henson teaches that the use of random characters to pad encrypted data is advantageous since it provides for better concealing the encrypted data in storage (Henson Col 12 lines 1-9).

25. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Henson with those of the above combination for a more secure system by better concealing the encrypted data as denoted by Henson.

26. Regarding Claim 3: Storage means contains random bit patterns (Henson Col 12 lines 1-9).

Conclusion

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Applicant is reminded that in amending in response to a rejection of claims, the patentable novelty must be clearly shown in view of the state of art disclosed by the references cited and the objections made. Applicant must show how the amendments avoid such references and objections. See 37 CFR 1.111(c).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Szymanski whose telephone number is 571-272-8574. The examiner can normally be reached on M-F 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TMS
2/27/2007

KAMBIZ ZAND
PRIMARY EXAMINER